

EX PARTE OR LATE FILED

LAW OFFICES

KELLER AND HECKMAN

1001 G STREET, N.W.
SUITE 500 WEST
WASHINGTON, D.C. 20001
TELEPHONE (202) 434-4100
TELEX 49 95551 "KELMAN"
TELECOPIER (202) 434-4646
BOULEVARD LOUIS SCHMIDT 87
B-1040 BRUSSELS
TELEPHONE 32(2) 732 52 80
TELECOPIER 32(2) 732 53 92

JOSEPH E. KELLER
JEROME H. HECKMAN
WILLIAM H. BORGHESEANI, JR.
MALCOLM D. MACARTHUR
WAYNE V. BLACK
TERRENCE D. JONES
MARTIN W. BERCOVICI
JOHN S. ELDRID
RICHARD J. LEIGHTON
ALFRED S. REGNIER
WILLIAM L. KOVACS
CAROLE C. HARRIS
DOUGLAS J. BEHR
RAYMOND A. KOWALSKI*
MICHAEL F. MORRONE
JOHN B. RICHARDS
JEAN SAVIGNY*
JOHN B. DUBECK
PETER L. DE LA CRUZ
CHRISTINE M. GILL
MELVIN S. DROZEN
SHIRLEY S. FUJIMOTO
LAWRENCE P. HALPRIN
RALPH A. SIMMONS

RICHARD F. MANN
PETER A. SUBSER
C. DOUGLAS JARRETT
SHEILA A. MILLAR
GEORGE G. MISKO
PATRICK J. HURD
GAREN E. DODGE
DAVID I. READER
SUSAN ANTHONY
MARK A. SIEVERS
MICHAEL R. BENNETT
DAVID G. SARVADI*
CATHERINE R. NIELSEN
KRIS ANNE MONTEITH
AMY N. RODGERS
ELLIOT BELLOS
MARK L. ITZKOFF
MARC BEREJKA
JEAN-PHILIPPE MONTFORT*
ARCHIE L. HARRIS, JR.
T. PHILLIPS BECK
ARTHUR S. GARRETT III
RICK D. RHODES
LESLIE E. SILVERMAN

FRANK C. TORRES III
BRYANT ROBINSON III
JOSEPH M. SANDRI, JR.
ELIZABETH F. NEWBILLO
TAMARA Y. DAVIS
ROBERT H. G. LOCKWOOD
CAROL MOORS TOTH
JOAN C. SYLVAIN
MARTHA PELLEGRINI*
BARRY J. CHILSON*
DONALD T. WURTH
DAVID B. BERRY
STEPHEN V. KENNEY
S. DEBORAH ROSEN*
DAVID R. JOY*
FREDERICK A. STEARNS*
DOROTHY ERSTLING CUKIER*
TONYE RUSSELL EPPS*
THOMAS C. BERGER*
JOHN P. FOLEY*

SCIENTIFIC STAFF
DANIEL S. DIXLER, Ph. D.
CHARLES V. BREDER, Ph. D.
ROBERT A. MATHEWS, Ph. D.
JOHN P. MODDERMAN, Ph. D.
HOLLY HUTMIRE FOLEY
JUSTIN C. POWELL, Ph. D.
JANETTE HOUK, Ph. D.
LESTER BORODINSKY, Ph. D.

TELECOMMUNICATIONS
ENGINEER
CHARLES F. TURNER

*NOT ADMITTED IN D.C.
RESIDENT BRUSSELS

WRITER'S DIRECT DIAL NUMBER

July 8, 1994

(202) 434-4233

RECEIVED

JUL 8 1994

HAND-DELIVERED

EX PARTE NOTICE

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W.
Room 222
Washington, D.C. 20554

Re: Ex Parte Presentation
CC Docket No. 93-292
Toll Fraud Proceeding

Dear Mr. Caton:

Transmitted herewith, on behalf of the Telecommunications
Committee of the American Petroleum Institute ("API"), and in
accordance with Section 1.1206 of the Rules and Regulations of
the Federal Communications Commission, are two copies of a
written ex parte presentation delivered this date to the
following Commission officials:

- The Honorable Reed E. Hundt, Chairman
The Honorable Andrew C. Barrett, Commissioner
The Honorable James A. Quello, Commissioner
The Honorable Rachelle B. Chong, Commissioner
The Honorable Susan Ness, Commissioner
Richard Metzger, Jr., Acting Chief, Common Carrier Bureau
Kathy Levitz, Deputy Chief (Policy), Common Carrier Bureau
Ruth Milkman, Sr. Legal Advisor to Chairman Hundt
Lauren Belvin, Sr. Legal Advisor to Chairman Quello
Byron F. Marchant, Sr. Legal Advisor to Commissioner Barrett
Jane Mago, Sr. Advisor to Commissioner Chong
James L. Casserly, Sr. Advisor to Commissioner Ness
Linda Dubroof, Common Carrier Bureau

No. of Copies rec'd
List ABCDE

001

Mr. William F. Caton
July 8, 1994
Page 2

KELLER AND HECKMAN

Should you have any questions or require additional information, please feel free to contact the undersigned.

Sincerely,

A handwritten signature in cursive script that reads "Michael R. Bennet".

Michael R. Bennet

Enclosures

EX PARTE OR LATE FILED

RECEIVED

American Petroleum Institute
1220 L Street, Northwest
Washington, D.C. 20005
202-682-8000



JUL 8 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

July 8, 1994

The Honorable Reed Hundt
Chairman
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

Dear Chairman Hundt:

Toll fraud is a continuing concern for telecommunications users. Unscrupulous persons are alarmingly successful in compromising PBX systems and in securing unauthorized access to the public switched network. Many companies have incurred tens of thousands of dollars in toll fraud losses.

In an effort to prevent such abuses and exchange information, the American Petroleum Institute's Telecommunications Committee formed a task force to study the matter and make recommendations. Enclosed for your review is a copy of this group's report, entitled "Toll Fraud Prevention Guidelines" (alternatively referred to as "Guidelines" or "the Study").

The Study is based on the experience of API member companies. It identifies the principal pathways by which hackers access and compromise PBX systems and sets forth guidelines and specific recommendations to minimize toll fraud. In compiling the Guidelines, the task force noted two recurring themes. First, hackers will attempt to devise new and more sophisticated schemes to compromise PBX systems. Second, carriers, equipment manufacturers, equipment support organizations, and users must take proactive approaches to minimize toll fraud.

API is a party to the Commission's toll fraud proceeding, CC Docket No. 93-292¹. Consistent with the conclusion of its toll fraud task force that a proactive response is essential, API's Comments urged the Commission to adopt a scheme of shared liability in order to ensure appropriate incentives exist for all parties to act responsibly and proactively to minimize the likelihood and extent of toll fraud. See CC Docket No. 93-292, API Comments, pages 3-17.

¹ A copy of this letter and the Guidelines are being filed concurrently with the Secretary as a written ex party presentation in CC Docket No. 93-292.

We are forwarding these Guidelines to you and the Commission to advance the ongoing dialogue on toll fraud by highlighting the proactive steps that users can take. API urges the Commission to call upon equipment manufacturers, equipment maintenance organizations, and carriers to present and describe fully the proactive steps they are instituting to prevent toll fraud and minimize toll fraud losses.

Very truly yours,



Sam R. Scroggins
Mobil Oil Corporation
Chair, Common Carrier Subcommittee
API Telecommunications Committee

cc: The Honorable James A. Quello, Commissioner
The Honorable Andrew C. Barrett, Commissioner
The Honorable Rachelle B. Chong, Commissioner
The Honorable Susan Ness, Commissioner
Richard Metzger, Jr., Acting Chief, Common Carrier Bureau
Kathy Levitz, Deputy Chief (Policy), Common Carrier Bureau
Ruth Milkman, Sr. Legal Advisor to Chairman Hundt
Lauren Belvin, Sr. Legal Advisor to Commissioner Quello
Byron F. Marchant, Sr. Legal Advisor to Commissioner Barrett
Jane Mago, Sr. Advisor to Commissioner Chong
James L. Casserly, Sr. Advisor to Commissioner Ness
Linda Dubroof, Common Carrier Bureau



American Petroleum Institute

Telecommunications Committee

Toll Fraud Prevention Study

April 1994

PREFACE

Acknowledgements

API member companies contributing materials:

- AMOCO Corporation - *Telephone System Security Guidelines*, published January 1992.
- Atlantic Richfield Company - Descriptive memorandum, published by Control and Audit, November 1992.
- Chevron Corporation - *Recommendations to Control Toll Fraud*, published April 1992.
- Occidental Petroleum Services - *Toll Fraud Awareness*, September 1992.
- Texaco Exploration and Production, Inc. - *Telecommunications Security Bulletin #1*, June 1991.
- Chevron Corporation - Toll Fraud Control Checklist, Published January 1993.
- Occidental Petroleum Services - PBX Fraud Review Checklist, Published May 1993.
- Marathon Oil Company - Voice Telecommunications Audit Program, Published November 1992.

Compiled by: Mr. G. L. Wassmann and Mr. E. G. Wong, Chevron Corporation

Contact Information Regarding This Document

If there are any questions concerning this document, please contact:

Information Systems Director
American Petroleum Institute
1220 Street, N.W.
Washington, D.C. 20005
202-682-8364

Copyright

© Copyright 1994 American Petroleum Institute

**Base
Document
Date**

April 1993

Revision Date

April 1994

Foreword

**Purpose of
This
Document**

The purpose of this document is to provide information for API members to consider in protecting themselves against toll fraud. The information is derived from publications written by members of the API and represents a synthesis of their ideas and the author's experience.

Note

This document is for information purposes only, and is intended to be used by API member companies as they see fit. There is no guarantee that these recommendations are comprehensive or complete. Implementation of these recommendations is entirely at the discretion and good judgement of the reader.

Table of Contents

| | |
|--|----|
| 1 • Overview of Toll Fraud | 1 |
| 2 • Manage Responsibilities | 3 |
| 3 • Secure Access to the PBX System | 5 |
| 4 • Deny Fraudulent Use of the PBX | 9 |
| 5 • Inform and Train Clients | 13 |
| 6 • Monitor PBX Activities | 15 |
| 7 • Additional Comments | 17 |
| 8 • PBX Toll Fraud Examples | 21 |
| 9 • PBX Toll Fraud Prevention Checklist | 25 |
| 10 • Cellular Telephone Fraud Prevention | 37 |

1 • Overview of Toll Fraud

Introduction

The telephone systems and cellular telephones of members of the API and other companies in North America are under attack by criminals who seek to resell long distance telephone services they obtain by fraudulent means. The people engaged in this activity may be viewed as an industry, one that has annual sales in excess of one billion dollars. Losses for fraudulent toll charges at a vulnerable PBX may run to many thousands of dollars in a weekend. Losses totaling in the hundreds of thousands of dollars have been known to accumulate before the fraud was discovered and some corrective action taken.

Methods of PBX Toll Fraud

The most useful mechanism to perpetrate toll fraud involving PBX systems is a sneak path through the PBX that allows someone to call the PBX and then use a PBX facility to extend the call, free of charge to the perpetrator, to anywhere in the world. When these paths are associated with toll free 800 numbers to call the PBX, the fraudulent reseller is really into a money-making business. There are other ways to commit toll fraud that have to be dealt with, but the sneak path is the most attractive from the criminal view.

Sneak paths may be established inadvertently by the telephone system provider, or deliberately by a hacker who has penetrated the PBX system and who prepares a path by modifying the PBX software configuration options. While there have been no widely-publicized instances yet, it is obvious that a sufficiently-skilled hacker could modify the software code with the intent of perpetrating malicious mischief or tapping conversations to steal trade secrets. Hackers have turned professional: making money by selling their knowledge and services, and becoming more of a serious threat.

The threat of PBX toll fraud and hacker PBX penetrations should have the attention of a corporation's management since it is serious and should be dealt with accordingly.

Methods of Cellular Telephone Fraud

There are three types of telephone fraud:

1. Access Fraud
2. Subscription Fraud
3. Theft of Cellular Phones and Unauthorized Usage

Access fraud is the most sophisticated and most costly of the three types of fraud. Access fraud is committed by either randomly or sequentially changing

the Electronic Serial Number (ESN) and/or Mobile Identification Number (MIN) after every call. This constant tumbling of the ESN and/or MIN confuses the cellular computer just long enough to let an additional (unauthorized) call be made. Another method used is programming a valid MIN/ESN match into the cellular phone, hence appearing to the cellular phone computer to be a valid customer. The hacker places as many calls as possible before being detected. This method is also known in the cellular industry as counterfeiting or cloning.

Subscription fraud occurs when a subscriber signs up for service with fraudulently obtained customer information or false identification, without any intention to pay for the service.

Usage of stolen telephones is the theft and unauthorized use of a cellular telephone before the owner of the phone reports the theft.

Prevention

An approach to combatting this threat is described in the recommendations contained in the following sections. The approach is measurable on a PBX-by-PBX basis. In outline, it follows the section titles: Put capable people in charge with a clear responsibility to handle the situation, make the PBX hacker-proof by setting up barriers around the PBX, cleanse the PBX of sneak paths and other conditions that can support fraud or hacking, monitor the PBX to catch break-ins and fraud at early stages, and enlist clients in the effort through education to spot fraud, discourage hackers, and reduce system vulnerability.

The cellular telephone fraud prevention recommendations are contained in section 10.

2 • Manage Responsibilities

Overall Responsibility

Overall responsibility for telecommunications services may lie with a corporate telecommunications manager, the managers of the individual end-user business unit, or elsewhere depending on the corporation. These managers should be aware of the risks to the corporation of hackers attacking PBX systems, of the measures necessary to control these risks, and of the need to make judgements about controlling these risks.

Managing Responsibility

Fixing responsibility can be especially challenging when the equipment service provider is a contractor, rather than an in-house organization, since a widely-accepted division of liability for toll fraud and other acts has not been established in the telecommunications industry. The contractor should be willing to accept reasonable consequences of any failure on their part to control security and toll fraud when they accept the responsibility and rewards of providing service. Auditable measures to control security and toll fraud must be included in all new service contracts, and existing contracts upgraded where that is practical.

Specifications regarding system security and integrity must be a part of new procurement documents, together with requests for descriptions of what safeguards the equipment manufacturer has built into the product, what cautionary information they have regarding use of features that may be abused, and how the vendor will act to support system security and integrity.

Control

There are a number of areas where a manager must exert control; these include the listed items which are covered in greater detail in this document:

- Ensuring physical security of the PBX
 - Ensuring remote maintenance access security
 - Denying fraudulent use of the PBX
 - Informing and training the people who use the PBX
 - Monitoring of the PBX for security breaches
 - Monitoring of the PBX for fraudulent use
-

Auditing the System

Management should express their concerns in policies that can be audited. Scope of the audits should include vendor procedures and carrier billings as well as PBX controls. Checklists that would be incorporated in audits may, in part, be derived from the detailed recommendations in the following sections. Other sources of audit checklists specifically for PBX systems are training sessions held for corporate auditors and recent books on combatting toll fraud.

Within a corporate framework, published checklists and audits may be used to encourage compliance by end-user business units. Corporate Telecoms could offer a form of insurance against fraudulent loss for units that comply. Otherwise, the full risk of loss would remain with the business unit.

Communication In the Community

A final step is keeping in touch with the toll fraud control community, including the equipment vendors and the carriers. The purpose is to stay abreast of criminal methods and ways to combat them. Membership in a toll fraud control organization is a possibility.

Conclusion

Overall, management must understand the vulnerabilities of the PBX to fraudulent use and subversion, and take steps to reduce risk to acceptable levels.

3 • Secure Access to the PBX System

Introduction

The intent of securing access is to keep the hackers out of the system equipment and the system software. If they are not kept out, hackers will be able to subvert the system to their purposes. Hackers who gain access to the system software can modify software configuration options and invoke unused feature options to establish pathways for fraudulent calls. Additionally, a sufficiently skilled hacker could conceivably cause malicious mischief such as planting time bombs in the system code or tapping the calls of selected telephones by a silent conference. The key methods of control are a physical barrier around the PBX and a reliable authentication method on the system-remote maintenance access lines. This is supplemented by methods to keep knowledge about the system confidential.

Physical Barriers

The best approach is to provide a separate, dedicated room for the PBX to isolate it from the other building tenants. The PBX room should be locked and secured with a protected entry system such as a card reader or security guard. PBX service personnel, telephone company employees, and others that may have need to visit should be expected to get permission to visit the room ahead of time and to present credentials. Where practical, the telephone company interface should be in a separate space.

Physical security should extend to the wiring closets. These should be separate, lockable spaces; i.e., not combined with electrical closets or janitorial closets.

Remote Access Authentication

The typical remote-access arrangement is a modem on a PBX maintenance port in place of a local terminal with authentication by a password. In some older PBXs this was an easily-hacked short numeric password. Voice mail systems and other PBX adjuncts that have their own maintenance port also present avenues for hacking and subversion. Common minimum recommendations for passwords are:

- Six alphanumeric characters with eight characters or more preferred.
- Avoid common words or character strings, or vendor initial default passwords that are easily guessed.
- Use devices that will lock out a caller after failed attempts to authenticate; two attempts is often considered enough.

- Delay modem answering for four or more rings.
- Use "silent" prompts during authentication.

Other steps often advocated are multiple layers of passwords and callback by the modems. These features are available in "smart" modems and also part of alarm-traffic monitoring units and call-detail record storage devices that are often associated with PBX ports when there are centralized PBX operation systems. There are also modems or add-on devices available that support higher security approaches based on the Data Encryption Standard (DES).

Procedures

Good equipment can be defeated unless there are accompanying good procedures. This starts with knowing the systems, particularly including a count of all the remote-access arrangements. Some essential points are:

- Every PBX must have someone in charge of its security.
 - Access must be limited to real need.
 - Passwords must be changed regularly (at least quarterly, if not monthly), and whenever there is a change in personnel.
 - Security review must be built into station-change procedures and system-change procedures to head off potential compromise.
 - Security reviews must be conducted on a regular basis (at least annually).
 - There must be an appointed body, such as a network control center, to monitor and track events, and to receive security inquiries from clients.
 - Default passwords must be changed.
-

Information Control

Hackers and the people who support them do search for information that would be useful in cracking systems. Trash sifting, also called dumpster diving, apparently is a popular method. The objects are corporate telephone books, maintenance terminal printouts, manuals of various kinds, and so on. Another is just walking into equipment rooms or support areas to look for modem telephone numbers, passwords, and system details. Things to do include:

- Don't have notes and messages with sensitive information such as access codes and modem telephone numbers posted on the walls.
- Put away sensitive information, even in "secure" spaces when it is not in use or when outsiders are about.

- Treat corporate telephone books as sensitive information, especially disposal of old ones.
 - Shred printouts of system information.
 - Treat telephone bills as sensitive information and shred when discarding.
 - Treat equipment manuals as sensitive information.
-

This page intentionally left blank.

4 • Deny Fraudulent Use of the PBX

Overview

Current PBX systems have many processes and features that have been developed to meet the needs of clients. A few of these can or do provide pathways through the PBX that are exploited by the toll fraud community. Especially enticing, fraud par excellence according to some commentators, is the association or possibility of associating free access into the PBX via an 800 service trunk with an outgoing trunk that is able to call the world. These pathways must be closed or secured by a reliable authentication method. The hard part may be convincing clients that a favorite feature is an unacceptable financial risk and must be eliminated.

PBX Call Control

The person in charge of the PBX must be able to find out what pathways exist through the PBX and how they are controlled. The purpose in this is to determine whether the controls are sufficient and appropriate. Developing a general, English language overview of the PBX call control should be possible without getting bogged down in the technical details. Controls may exist in the software in several layers, especially if the PBX is part of a private corporate network with a uniform numbering plan. It is possible that appropriate controls exist in the highly-visible network-automatic route selection layer, but sneak paths are left open in the physical "allowed connection" layer and the "basic class of service" layer.

Call Denial

Concern about call control has led to a large number of specific recommendations as noted below. These should be treated as examples with others added as needed. Whether these are appropriate to a particular PBX is a matter of judgement.

- Deny DID trunks access to outgoing trunks.
- Block 9 + 0 dialing by extensions.
- Restrict calling to common or hot spot toll fraud destinations (for example, the 809 area code serving Puerto Rico, Dominican Republic, etc.).
- Block 900, 976, and 700 calls.
- Block call transfer to the outside.
- Control trunk-to-trunk transfer.

- Control direct trunk access.
 - Set network class of service and facility restriction levels low.
 - Block 800 calls from areas that are fraud hot spots (parts of New York City).
 - Verify PBX routing tables and clean out unneeded pathways.
 - Don't use common "level" numbers (8, 9, etc.) for direct trunk access codes.
 - Review routing tables frequently for unneeded mechanisms.
-

**Direct Inward
Station
Access
(DISA)
Feature**

The DISA feature has been under heavy attack by the toll fraud community, so much so the general recommendation has become to abandon use of the feature. Frequently an 800 number is associated with DISA, so that traveling salesmen and others have a convenient way to use the corporate network. Passwords implemented with this feature, even multilayer passwords, are often short, have easily guessed character combinations, and are infrequently changed. This is a recipe for disaster. The recommended alternative is telephone calling cards. An attractive feature of calling cards is the limit of fraudulent call liability that exists by legislation. If DISA must be retained, it must be guarded by a reliable authentication method. At minimum, very long passwords must be used. A method involving the use of a small hand-held personal identification device based on procedures described in the Data Encryption Standard (DES) may be more convenient in some situations.

**Voice Mail
Through-Dial**

This is a feature that can be used very much like DISA - following directions of the voice mail box greeting, a caller may be enabled to extend their call outside of the PBX. Even if the feature is thought to be limited to calls within the PBX, clever hackers will explore the PBX dial plan for flaws leading to the outside. The general recommendation is to not use this feature. However, if it must be used, then on a conditional basis as follows:

- Calls are allowed only to fixed destinations autodialed by the voice mail system, such as to a paging system or car phone.
- There is a positive disconnect sequence all the way through the PBX when the called party hangs up first.
- If used to extend calls to inside PBX parties, the voice mail outgoing lines (connect to incoming PBX lines) must be constrained to deny long-distance calls, and the basic call-control scheme in the PBX must be cleaned up.

- The mailbox password must be resistant to hacking - initial or default changed, long, no easily guessed character patterns, and changed often.
 - The mailbox greeting must not provide clues to the PBX numbering plan.
-

Automated Attendant

The PBX may be equipped with an automated attendant which is a dial-controlled robot that redirects calls into the PBX, handles elementary information requests, and so on. These may be inadvertently, or deliberately, programmed to provide or support the same kind of connections as DISA. Their use must be examined very carefully, especially if an 800 number is used to reach the automated attendant.

External Call Forwarding

Call forwarding is a very popular feature of current PBX systems. One method of abuse by employees is to forward their telephone to outside trunk dial tone after hours enabling personal calls or legitimate business calls from home. These lines are sought by hackers. The recommendation is to withdraw this feature unless there are very special circumstances.

Call Diverters

These are used to forward calls to a call-answering service. They may be abused in some public networks by a hacker arguing the answering service into hanging up first. If the PBX doesn't sense the answering service disconnect and disconnect in turn, the hacker can redirect the call to anywhere in the public network. The general recommendation is to establish these arrangements with care, ensuring that complete disconnect occurs in all circumstances.

Voice Mail Mailboxes

Mailboxes may be subverted by hackers and turned to their purposes, such as running bulletin boards, sometimes with some larger criminal purpose in mind. To prevent this, the "owner" of the mailbox must use due diligence:

- The owner must use good password procedures.
 - The system administrator should, if practical, force the change of initial passwords (typically the telephone number), to a recommended minimum length. Periodic change of passwords should also be forced.
 - The system administrator should remove unused mailboxes.
-

**Referred
Charges**

Toll fraud may occur by people making third-party calls with charges referred to station numbers in the PBX. While the telephone company handling the call request is required to confirm acceptance of the charges with the third party, some are not diligent in the pursuit of this. Employees may also be accepting collect calls against the wishes of the management, or be duped into accepting charges by criminals using "social engineering" techniques (i.e., to gain access to a system by "sweet talk," or by a predictable reaction to "harsh talk"). Modern central office telephone systems can be programmed to automatically reject third-party and collect calls when attempted by a toll operator if the PBX administrator makes the request of the telephone company. Such requests should be in writing and maintained on file to provide a basis for claiming rebates if these charges occur or continue. Third-party and collect calls can be handled separately. Detection of such activities may require close examination of telephone bills; if taking place at a low level, they may persist for long periods.

5 • Inform and Train Clients

Introduction End-user management, system attendants, and clients themselves must be aware of the dangers of toll fraud and be informed of how to prevent it. This often can be made a part of other training and reinforced in publications.

Awareness Training A key issue for all parties is how to prevent becoming a victim of “social engineering,” for example:

- Be cautious of people impersonating someone who has “forgotten” the PBX password.
- Be cautious of people who seem to have gotten “lost” in the system and want to be transferred.
- Practice password discipline for voice mailbox use. Provide only appropriate information in the greeting.

Physical Barriers The attendants and others involved in close support of the PBX must know of the need to maintain physical barriers around the PBX and the procedures that have been established to accomplish this. There must also be convenient procedures at the client level to report possible telephone security incidents with follow-up that includes feedback to the reporting party.

This page intentionally left blank.

6 • Monitor PBX Activities

Overview

Constant monitoring of the internal environment of the PBX and the external trunk environment is necessary to "close the loop" on earlier recommendations in order to discover new fraud and to find fraud that may be ongoing despite best efforts to secure the PBX. Monitoring essentially means watching in near real time the PBX traffic peg counts for unusual trunk activity, and observing the call detail record (CDR) data stream for high-cost calls to unusual destinations. This can be done by currently-available alarm systems that report to central sites that are 24-hour operations. The CDR data stream may be less reliable than traffic peg counts. A hacker who has subverted the PBX may shut off CDR collection, or the call path arrangement may not require the PBX to repeat the dialed information and so escape CDR collection.

Establishing a Baseline

Performing studies on traffic and other system parameters to establish a baseline before any new efforts to tighten security or control potential fraud may be useful in determining whether some unnoticed ongoing fraud existed.

Routine Monitoring

Many commentators recommend daily examination of CDR information, but this can be quite labor-intensive and unlikely to be a prolonged activity unless there are automated means to do the examination. Near real-time examination is essential, otherwise the fraudulent activity may have taken its toll and gone before it is spotted, and all that has happened is discovery of the size of the bill a little before it arrives.

A working arrangement with the carriers to detect unusual activity and notify someone who can respond by checking the PBX is a good approach if it can be established with all carriers, including the ones not normally getting the corporation's business, and is affordable.

This page intentionally left blank.